REMARKS

The Specification has been amended. Claims 1, 3, 6, 8, 12, and 14 - 15 have been amended. No new matter has been introduced with these amendments, all of which are supported in the application as originally filed. Claims 2, 4 - 5, 7, 9 - 11, 13, and 16 - 21 have been cancelled from the application without prejudice. Claims 1, 3, 6, 8, 12, and 14 - 15 remain in the application.

Applicants are not conceding that the subject matter encompassed by the claims as presented prior to this Amendment is not patentable over the art cited by the Examiner, and claim amendments and cancellations in the present application are directed toward facilitating expeditious prosecution of the application and allowance of the currently-presented claims at an early date. Applicants respectfully reserve the right to pursue claims, including the subject matter encompassed by the claims as presented prior to this Amendment and additional claims, in one or more continuing applications.

I. Objection to the Specification

Paragraph 3 of the Office Action dated April 15, 2008 (hereinafter, "the Office Action") states that the Specification is objected to as failing to provide proper antecedent basis for Claim 18. Claim 18 has been cancelled from the application without prejudice, rendering this objection moot.

II. Rejection under 35 U. S. C. §112, second paragraph

Paragraph 5 of the Office Action states that Claim 19 is rejected under 35 U.S.C. §112, second paragraph, as being indefinite. Claim 19 has been cancelled from the application without prejudice, rendering this rejection moot.

III. Rejection under 35 U. S. C. §101

Paragraph 7 of the Office Action states that Claims 17 - 18 are rejected under 35 U.S.C. §101 as being directed to non-statutory subject matter. Claims 17 - 18 have been cancelled from the application without prejudice, rendering this rejection moot.

IV. Rejection under 35 U. S. C. §103(a)

Paragraph 9 of the Office Action states that Claims 1 - 21 are rejected under 35 U.S.C. §103(a) as being unpatentable over U. S. Patent 7,130,885 to Chandra et al. (hereinafter, "Chandra") in view of "Global Convergence of Telecommunications and Distributed Object Computing", a publication of Hamada (hereinafter, "Hamada"). Claims 2, 4 - 5, 7, 9 - 11, 13, and 16 - 21 have been cancelled from the application without prejudice, rendering the rejections moot as to those claims. This rejection is respectfully traversed with regard to remaining Claims 1, 3, 6, 8, 12, and 14 - 15 as currently presented.

Independent Claim 1, as currently presented, recites:

> A computer-implemented method of achieving context-sensitive confidentiality among security domains within a federated environment that

spans a plurality of security domains, the method comprising:

determining a route to be taken by a content request message to be transmitted from a content requester in the federated environment to a content provider in the federated environment, wherein:

the route comprises a network transmission path which begins at the content requester and ends at the content provider and passes through a plurality of intermediary nodes, each of the intermediary nodes located between the content requester and the content provider on the network transmission path;

the route is determined by consulting stored policy that specifies, for the content receiver sending the content request message to the content provider, the network transmission path; and

the route spans a plurality of the security domains;

storing the determined route at a network-accessible location;

determining, prior to transmitting the content request message from the content requester, a plurality of portions of the content request message that are security-sensitive, further comprising using a context to consult stored policy that identifies the security-sensitive portions which are applicable to that context, wherein the context comprises an identification of the content requester, an identification of the content provider, and a message type identifying the content request message;

determining, prior to transmitting the content request message from the content requester, rights of each of the intermediary nodes to access each of the determined security-sensitive portions of the content request message, further comprising consulting stored policy for each of the intermediary nodes, wherein the stored policy specifies whether this intermediary node is entitled to access this security-sensitive portion of the content request message;

specifying, in unencrypted form in the content request message, the message type; an identifier of the network-accessible location where the determined route is stored; and a plurality of message receiver elements, wherein a separate one of the message receiver elements is specified for each of the intermediary nodes that is entitled to access each of the security-sensitive portions, the separate one specifying an identification of that intermediary node as a permitted receiver of that security-sensitive portion and a node-specific keyword corresponding to that intermediary node;

selectively protecting the security-sensitive portions of the content request message, according to the determined access rights by encrypting, for each of the security-sensitive portions of the content request message, that security-sensitive portion separately for each distinct one of the intermediary nodes which is entitled to access that security-sensitive portion and storing that separately-encrypted security-sensitive portion in the content request message in association with the node-specific keyword corresponding to that distinct one

> of the intermediary nodes, thereby enabling each of the intermediary nodes to locate and access each of the security-sensitive portions which it is entitled to access and preventing that intermediary node from accessing any of the security-sensitive portions which it is not entitled to access; and
>
> transmitting the content request message with its selectively-protected portions from the content requester to the content provider on the determined route, wherein:
>
> the transmitted content request message contains information identifying an authentication authority from a first of the security domains and an identification of a party for which the content request message requests access to services and indicates that the identified authentication authority has already authenticated the party using security credentials of the party in the first security domain;
>
> the intermediary nodes and the content provider, upon receiving the content request message in other ones of the security domains, can bypass authentication of the party for access to services of that other security domain, upon verifying authenticity of the authentication authority, establishing that the authentication authority vouches for the received content request message, and using the identification of the party to locate previously-stored security credentials for the party which are usable within that other security domain; and
>
> the security credentials for the party in at least one of the other security domains are different from the security credentials of the party in the first security domain. (emphasis added)

Applicants respectfully submit that neither Chandra nor Hamada teaches or suggests at least the above-underlined recitations of independent Claim 1.

With reference to the "specifying, in unencrypted form ..." element recited at lines 28 - 34 of Claim 1, this is illustrated in **Fig. 5** at reference number **510** (for the claimed "identifier of the network-accessible location ...") and in **Fig. 6** at reference numbers **605** (for the claimed "message type") and **615**, **620** (for the claimed "separate one of the message receiving elements ..."). Corresponding text is found in paras. **[0066]** and **[0079]** of Applicants' specification.

The "selectively protecting ..." element recited at lines 35 - 44 of Claim 1 is illustrated in **Fig. 6** at references numbers **625**, **630**, each of which shows an "... encrypting, for each of the security-sensitive portions ... that security-sensitive portion separately ... and storing that separately-encrypted ... portion ... in association with the node-specific keyword ..." (where the node-specific keywords, in this example, are "1234Tag" and "RTPTag"). Corresponding text is found in paras. **[0078]** and **[0080]** through **[0082]** of Applicants' specification.

The "transmitting the content request message ..." element recited at lines 45 - 59 of Claim 1 is discussed in (at least) paras. **[0068]** and **[0072]** through **[0073]** of Applicants' specification.

Accordingly, Applicants respectfully submit that the §103 rejection is overcome with regard to independent Claim 1. Dependent Claims 3, 6, 8, 12, and 14 - 15 are deemed patentable by virtue of at least the patentability of Claim 1 from which they depend.

The Examiner is therefore respectfully requested to withdraw the §103 rejection.

V. <u>Conclusion</u>

Applicants respectfully request reconsideration of the pending rejected claims, withdrawal of all presently outstanding objections and rejections, and allowance of all remaining claims at an early date.

Respectfully submitted,

/Marcia L. Doubet/

Marcia L. Doubet,
Attorney for Applicants
Reg. No. 40,999

Cust. Nbr. for Correspondence: 43168
Phone: 407-343-7586
Fax: 407-343-7587